AF

TRANSMITTAL

PATENT

Application No.: 09/659,864
Filing Date: September 12, 2000
First Named Inventor: J. Leslie Vogel, III
Examiner's Name: Tongoc Tran
Art Unit: 2134
Attorney Docket No.: 004860.P2436

____ An Amendment After Final Action (37 CFR 1.116) is attached and applicant(s) request expedited action.
__X__ Charge any fee not covered by any check submitted to Deposit Account No. 02-2666.
__X__ Applicant(s) hereby request and authorize the U.S. Patent and Trademark Office to (1) treat any concurrent or future reply that requires a petition for extension of time as incorporating a petition for extension of time for the appropriate length of time and (2) charge all required fees, including extension of time fees and fees under 37 CFR 1.16 and 1.17, for any concurrent or future reply to Deposit Account No. 02-2666.
____ Applicant(s) claim small entity status (37 CFR 1.27).

ATTACHMENTS

____ Preliminary Amendment
____ Amendment/Response with respect to Office Action
____ Amendment/Response After Final Action (37 CFR 1.116) (reminder: consider filing a Notice of Appeal)
____ Notice of Appeal
____ RCE (Request for Continued Examination)
____ Supplemental Declaration
____ Terminal Disclaimer (reminder: if executed by an attorney, the attorney must be properly of record)
____ Information Disclosure Statement (IDS)
____ Copies of IDS citations
____ Petition for Extension of Time
____ Fee Transmittal Document (that includes a fee calculation based on the type and number of claims)
____ Cross-Reference to Related Application(s)
____ Certified Copy of Priority Document
__X__ Other: Supplemental Appeal Brief Under 37 C.F.R. §41.50(d)
____ Other: ____
____ Check(s)
__X__ Postcard (Return Receipt)

SUBMITTED BY:

BLAKELY SOKOLOFF TAYLOR & ZAFMAN LLP
TYPED OR PRINTED NAME: Sheryl Sue Holloway
SIGNATURE:
REG. NO.: 37,850
DATE: Aug. 21, 2007
ADDRESS: 1279 Oakmead Parkway
Sunnyvale, CA 94085-4040
TELEPHONE NO.: (408) 720-8300

CERTIFICATE OF MAILING BY FIRST CLASS MAIL (if applicable)

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail with sufficient postage in an envelope addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria Virginia 22313-1450
on 8.21.07
Date of Deposit
Carla Anysia Nascimento
Name of Person Mailing Correspondence
Signature
8.21.07
Date

Express Mail Label No. (if applicable): ____

(10/14/03)

Send to: COMMISSIONER FOR PATENTS, P.O. Box 1450, Alexandria, Virginia 22313-1450

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of:	)	Examiner: Tran, Tongoc
Vogel, J. Leslie III	)	Art Unit: 2134
Application No. 09/659,864	)	Confirmation No.: 5866
Filed: September 12, 2000	)	
For: USER CONTROL OF A SECURE WIRELESS COMPUTING NETWORK	)	

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

SUPPLEMENTAL APPEAL BRIEF UNDER 37 C.F.R. § 41.50(d)

This supplement appeal brief is in response to the Board's request on July 23, 2007 for further information under 37 C.F.R § 41.50(d)(2006). Applicant is submitting a supplemental appeal brief because the information added under the Summary of Invention section changes the pagination of the original brief.

I. REAL PARTY IN INTEREST

The real party in interest is the assignee of the full interest in the invention, Apple Computer, Inc., Cupertino, CA.

II. RELATED APPEALS AND INTERFERENCES

To the best of Appellant's knowledge, there are no appeals or interferences related to the present appeal that will directly affect, be directly affected by, or have a bearing on the Board's decision in the instant appeal.

III. STATUS OF THE CLAIMS

Claims 1-51 are pending in the application and were rejected in a final Office Action mailed February 17, 2006. Claims 1-51 are the subject of this appeal. A copy of Claims 1-51 as they stand on appeal are set forth in the Claims Appendix.

IV. STATUS OF AMENDMENTS

No amendments to the claims have been made after receipt of the final Office Action on February 17, 2006.

V. SUMMARY OF CLAIMED SUBJECT MATTER

Appellant's invention as claimed in claims 1-51 is a wireless communication network. Claims 1-15, 36-41 and 46-51 claim an access point and a station operating together (Specification: page 10, line 14 through page 14, line 10 and Figure 2). Claims 16-20 and 26-30 claim one embodiment of a station (Specification: page 15, line 6 through page 16, line 2, page 16, line 18 through page 18, line 9, and Figures 3A and 3B). Claims 21-25 and 31-35 claim one embodiment of an access point (Specification: page 16, line 3 through page 18, line 9, and Figures 4A and 4B). Claims 42-45 claim a data structure for messages exchanged between an access point and a station (page 19, line 9 through page 21, line 7, and Figures 2 and 5).

A particular security algorithm claimed in claims 4, 8, 23 and 28 is described on page 18, lines 1-7 in conjunction with formulas 2-5 also shown on those pages.

Claims 46-51 are claims under 35 U.S.C. § 112, sixth paragraph, that recite an apparatus comprising a means for accessing and a means for messaging. The corresponding structure for the means for accessing is access point 203 of Figure 2; the corresponding structure for the means for messaging is station 201 of Figure 2. As claimed in independent claim 46, the means for accessing 203 receives a connection request 207 from a means for messaging 201 through a setup connection, and sends a security preference 209 that specifies one authentication protocol from a set of authentication protocols supported by the means for accessing 203 (page 11, lines 4-7). The setup connection comprises the connections 205, 211 and 221 as described on page

12, line 9. Support of multiple authentication protocols by the means for accessing is described on page 19, lines 1-5. The means for accessing 203 further validates authentication information 217 sent by the means for messaging 201 as described on page 12, lines 4-5. The means for messaging 201 is connected to the wireless network 223 through a channel secured with a shared channel key as described on page 12, lines 8-11. As claimed in independent claim 46, the means for messaging 201 sends the connection request 207 to the means for accessing 203 as described on page 11, line 6, and generates the authentication information 217 to send to the means for accessing 203 as described on page 12, lines 1-4.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

I. Claims 1, 16, 21, 26, 31, 36, 42 and 46 stand rejected under 35 U.S.C. § 112, first paragraph for lack of written description.

II. Claims 1, 16, 21, 26, 31, 36, 42 and 46 stand rejected under 35 U.S.C. § 102(a) over Patiyoot, et al. ("Technique for authentication protocols and key distribution on wireless ATM networks", ACM SIGOPS Operating System Review, Volume 32, Issue 4, October 1998).

III. Claims 1-3, 9-17, 19-22, 24-27, 29-32, 34-38, 40-48 and 50-51 stand rejected under 35 U.S.C. § 103(a) over Lewis, U.S. Patent No. 6,526,506, in view of Quick Jr., U.S. Patent No. 6,178,506.

IV. Claims 4-8, 18, 23, 28, 33, 39, and 49 are rejected under 35 U.S.C. 103(a) over Lewis and Quick in view of Schneier ("Applied Cryptography, Second Edition, Protocols, Algorithms, and Source Code in C", John Wiley & Sons, Inc., 1996).

VII. ARGUMENTS

I. Claims 1, 16, 21, 26, 31, 36, 42 and 46 are supported by the Specification under with 35 U.S.C. § 112, first paragraph.

Claims 1, 16, 21, 26, 31, 36, 42 and 46 stand or fall together. Claim 1 is the representative claim with respect to this § 112 rejection. Claim 1 claims a method of establishing secure wireless communications channel between an access point and a station, where the channel is encrypted with a channel key. The station requests a security preference from the access point. In response, the access points sends the security preference, which is one of a set of authentication protocols supported by the access point.

The Examiner asserts that Appellant's Specification does not disclose more than one authentication protocol, i.e., security preference. Appellant respectfully directs the Board's attention to page 10, line 20 through page 11 of Appellant's Specification that sets forth one example of a security preference as being "shared key." Other types of authentication for wireless networks, such as "open system," may be the security preference for a particular network as disclosed on line 7 and page 19, lines 1-5 of Appellant's Specification. Appellant respectfully submits that "open system" and "shared key" are well-known authentication protocols in the wireless networking art. In support of Appellant's assertion, Appellant is submitting, in the attached Evidence Appendix, the section 8.1f IEEE 802.11 standard, which states that both "open system" and "shared key" are authentication services and further specifies the particular message frames that form the protocols for the two authentication services.

Furthermore, Appellant specifically pointed to page 19, lines 1-5 of the Specification as supporting the claim amendments in the RCE mailed November 28, 2005. In the final Office Action mailed February 17, 2006, the Examiner did not even address Appellant's statement that the amendments were supported by the cited section. Thus, the Examiner has not established a proper *prima facie* case under § 112, first paragraphs, which requires reasons as to why someone of skill in the art would not have

recognized that the inventor was in possession of the claimed invention by reading Appellant's Specification.

Because claim 1 is supported by the Specification, Appellant respectfully submits that claims 1, 16, 21, 26, 31, 36, 42 and 46 satisfy the written description requirement of 35 U.S.C. § 112, first paragraph.

II. Claims 1, 16, 21, 26, 31, 36, 42 and 46 are patentable under 35 U.S.C. § 102(a) over Patiyoot.

Claims 1, 16, 21, 26, 31, 36, 42 and 46 stand or fall together. Claim 1 is the representative claim with respect to this § 102(a) rejection.

Patiyoot discloses using a public-private key pair authentication protocol to authenticate a wireless ATM terminal (WAT) to a wireless ATM server (WAS). Patiyoot discloses that the WAS only supports a single authentication protocol.

Thus, Patiyoot does not teach or suggest an access point sends a security preference that is one of a set of authentication protocols supported by the access point as claimed in claim 1.

Because Patiyoot does teach or suggest Appellant's invention as claimed in claim 1, Appellant respectfully submits that claims 1, 16, 21, 26, 31, 36, 42 and 46 are patentable under 35 U.S.C. § 102(a) over Patiyoot.

III. Claims 1-3, 9-17, 19-22, 24-27, 29-32, 34-38, 40-48 and 50-51 are patentable under 35 U.S.C. § 103(a) over the combination of Lewis and Quick.

Lewis discloses a multi-tiered encryption scheme for a wireless network. The first level of encryption is employed between a mobile device and access points on the network. The second level of encryption is employed between the mobile device and a key distribution server. When a mobile device wants to connect to an access point, the mobile device requests the current network encryption key from the key distribution server. The request and the response containing the network encryption key are encrypted with a master key. The access point can also send a new network encryption key to connected mobile devices in response to the key distribution server changing the network encryption key. The access point encrypts the new network encryption key with

the old network encryption key. Thus, Lewis discloses an access point that uses a single authentication protocol, i.e., the shared network encryption key.

Quick discloses a subscription service that is portable among different mobile devices. A mobile device generates a public/private key pair from the user's subscription identifier and password. The public key is encrypted with the password. All or part of the unencrypted identifier and the encrypted public key are sent to a server that is local to the mobile device's current location. The local server uses the unencrypted identifier to determine the user's home server and sends the encrypted public key to the home server for decryption. The mobile device is authentic if the decrypted public key matches the public key of the user stored on the home server. Further communication establishes the authentication of the home server to the mobile device. Once both ends of the link are authenticated, credentials can be passed to the mobile device to allow it to register with the local server and obtain an authentication key for the local server. Thus, Quick discloses that the home server and the local server each use a single authentication protocol: the home server shares a public/private key pair with the mobile device while the local server shared an authentication key with the mobile device.

A. Claims 1-3, 9-17, 19-22, 24-27, 29-32, 34-38, 40-42, 46-48 and 50-51

Claims 1-3, 9-17, 19-22, 24-27, 29-32, 34-38, 40-42, 46-48 and 50-51 stand or fall together. Claim 1 is the representative claim for this § 103(a) rejection.

Appellant claims an access point that supports a set of authentication protocols. As argued above, both Lewis and Quick's inventions support only a single authentication protocol for an access point.

Appellant also claims generating authentication information using a key. The Examiner asserts that Lewis' registration information is equivalent to Appellant's claimed authentication information, but Lewis does not teach or suggest that the registration information is generated using a key as claimed.

In addition, the Examiner continues to assert that Quick discloses Appellant's "claimed" encryption of the authentication information using a key. However, Appellant does not claim encrypting the authentication information. Instead, Appellant claims that the authentication information is <u>generated</u> using a first key. Appellant has repeatedly

pointed out the correct claim language to the Examiner but the Examiner continues to misstate the language of the claim in order to support his use of Quick to reject the claims. When the claim language is read properly it is readily apparent that Quick does not disclose Appellant's element as actually claimed. Quick's authentication information includes a public key, but Quick does not teach or suggest that the public key is generated using a key as claimed. In fact, Quick uses the Diffie-Hellman algorithm to generate the public key and the Diffie-Hellman algorithm is not key-based.

The Examiner is further equating Lewis' mobile device with Appellant's claimed station and Lewis' access point with Appellant's claimed access point. However, Lewis only discloses the exchange of network encryption keys, not security preferences as defined by Appellant. Moreover, even if Lewis' encryption key could be properly interpreted as equivalent to Appellant's claimed security preference, Lewis does not teach or suggest that the mobile device receives a new encryption key from the access point in response to the mobile device requesting the key. Instead in Lewis, the access point sends the new network encryption key to the mobile device in response to the access point receiving the new network encryption from the key distribution server. In fact, the mobile device cannot request a new network encryption key because it has no way of learning that the key distribution server has changed the key.

Nonetheless, the Examiner asserts that Lewis' access point is equivalent to Appellants access point because Lewis discloses an encryption engine resides in the access point, citing column 15, lines 25-34, Figure 1, block 54 (access point) and Figure 2, block 118 (encryption engine). However, the encryption engine 118 is described as only decrypting (col. 8, line 4-7) and encrypting messages (col. 15, lines 25-34). There is nothing in the cited sections of Lewis, or in Lewis as a whole, that suggest the encryption engine 118 sends a new network encryption key in response to a request from the mobile device. Thus, Lewis' access point cannot be properly equated with Appellant's claimed access point that does distribute a key in response to a request from a station.

Therefore, the combination of Lewis and Quick does not disclose each and every limitation claimed by Appellant for the station and access point in claim 1, and Appellant respectfully submits that claims 1-3, 9-17, 19-22, 24-27, 29-32, 34-38, 40-42, 46-48 and 50-51 are patentable under 35 U.S.C. § 103(a) over the combination.

B. Claims 42-45

Claims 42-45 stand or fall together. Claim 42 is the representative claim for this § 103(a) rejection and claims a data structure.

The Examiner has rejected claim 42 using the same arguments he uses to reject claims 1-3, 9-17, 19-22, 24-27, 29-32, 34-38, 40-42, 46-48 and 50-51. Appellant has repeatedly pointed out to the Examiner that neither Lewis nor Quick disclose any data structure, much less a data structure as claimed in claim 42. However, the Examiner continues to assert the same argument and has never acknowledged that Appellant is claiming a data structure or pointed to any disclosure in either reference that even suggests a data structure as claimed.

Because neither Lewis nor Quick teach or suggest the invention as claimed in claim 42, Appellant respectfully submits that claims 42-45 are patentable under 35 U.S.C. § 103(a) over the combination of Lewis and Quick.

IV. Claims 4-8, 18, 23, 28, 33, 39, and 49 are patentable under 35 U.S.C. 103(a) over the combination of Lewis, Quick and Schneier.

Claims 4-8, 18, 23, 28, 33, 39, and 49 stand or fall together. Claim 4 is the representative claim for this § 103(a) rejection and claims a particular security algorithm that is used to generate a key for the access point.

Schneier is directed toward various cryptographic processes. Because claim 4 depends from claim 1, Schneier must disclose the claimed elements that are missing from the combination of Lewis and Quick in order to have a proper *prima facie* case of obviousness. However, Schneier does not teach or suggest an access point that sends a security preference as claimed.

In the final Office Action dated February 17, 2006, the Examiner argued that the combination of Lewis, Quick and Schneier is proper. Appellant respectfully submits that Appellant has not challenged the validity of the combination during prosecution. Instead, Appellant has repeatedly pointed out that the Examiner has failed to state a proper *prima facie* case of obviousness because the combination does not teach each and every limitation of Appellant's claim 4. Since claim 4 includes all the limitations of claim 1, at

least one of the references must disclose an access point that sends a security preference as claimed in claim 1. However, none of the references disclose an access point as claimed.

Therefore, the combination of Lewis, Quick and Schneier does not teach each and every limitation of Appellant's invention as claimed in claim 4, and Appellant respectfully submits that claims 4-8, 18, 23, 28, 33, 39, and 49 are patentable under 35 U.S.C. § 103(a) over the combination.

VIII. CONCLUSION

Appellant respectfully submits that Appellant has overcome all the rejections of the pending claims. Therefore, Appellant respectfully requests the Board reverse the rejections of claims 1, 16, 21, 26, 31, 36, 42 and 46 under 35 U.S.C. § 112 and under 35 U.S.C. § 102 and the rejections of claims 1-51 under 35 U.S.C. § 103, and direct the Examiner to enter a Notice of Allowance for claims 1-51.

However, in the event the Board decides to remand the case to the Examiner for further prosecution, Appellant respectfully requests the Board instruct the Examiner to correct his misstatement of the language of the independent claims in subsequent Office Actions.

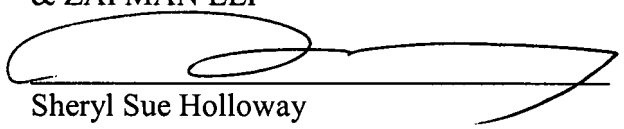
Fee for Filing a Brief in Support of Appeal

Applicant previously submitted a check in the amount of $500.00 to cover the fee for filing a brief in support of an appeal as required under 37 C.F.R. §§ 1.17(c) and 41.37(a) . Therefore, no additional fees are required.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR
& ZAFMAN LLP

Dated: August 21, 2007



Sheryl Sue Holloway
Attorney for Appellant
Registration No. 37,850

1279 Oakmead Parkway
Sunnyvale, CA 94085-4040
(408) 720-8300 x3476

CLAIMS APPENDIX FOR
APPEAL BRIEF UNDER 37 C.F.R. § 41.37

1. (Previously presented) A computerized method of establishing a secure wireless communications channel between an access point and a station, the channel being encrypted with a channel key, the method comprising:

sending, by the station to the access point through a setup connection, a request for a security preference for the access point;

sending, by the access point to the station through the setup connection, the security preference in response to the request when the access point can support the channel, wherein the security preference specifies one authentication protocol from a set of authentication protocols supported by the access point;

generating, by the station, authentication information using a first key when the security preference is shared key;

sending, by the station to the access point through the setup connection, the authentication information;

validating, by the access point, the station using the authentication information;

encrypting, by the access point, the channel key using a second key;

sending, by the access point to the station through the setup connection, the encrypted channel key;

decrypting, by the station, the channel key in response to receiving the encrypted channel key; and

sending, by the station to the access point, data encrypted with the channel key to establish the channel.

2. (Original) The method of claim 1, wherein the first and second keys are a self-distributed key.

3. (Original) The method of claim 2, further comprising:

generating, by the access point, the self-distributed key using a security algorithm when the security preference is shared key;

generating, by the station and sending to the access point, a first value using the security algorithm in response to receiving the security preference of shared key;

generating, by the access point, and sending to the station, a second value using the security algorithm and the first value in response to receiving the first value; and

calculating, by the station, the self-distributed key using the security algorithm and the second value in response to receiving the second value.

4. (Original) The method of claim 3, wherein the security algorithm is $g^n \bmod p$ and further comprising:

obtaining, by the access point, integers x, g and p to generate the self-distributed key $k = g^x \bmod p$;

obtaining, by the station, the integers g and p, and an integer y to generate the first value $Y = g^y \bmod p$;

generating, by the access point, the second value $X = Y^x \bmod p$; and

setting, by the station, z equal to y^{-1} to calculate the self-distributed key $k = X^z \bmod p$.

5. (Original) The method of claim 4 wherein obtaining, by the station, the integers g and p comprises:

sending, by the access point to the station, the integers for g and p.

6. (Original) The method of claim 5, wherein the integers for g and p are sent to the station when the security preferences are sent by the access point.

7. (Original) The method of claim 5, wherein the integers for g and p are sent to the station when a user name and password for the station are registered with the access point.

8. (Original) The method of claim 4 further comprising:

publishing, by the access point, the integers g and p for a set of stations.

9. (Original) The method of claim 2 further comprising:

encrypting, by the station, a name and password with the first key to generate the authentication information; and

decrypting, by the access point, the name and password to validate the station.

10. (Original) The method of claim 2 further comprising:

sending, by the access point to the station, a challenge;

encrypting, by the station, the challenge with the first key to generate the authentication information;

encrypting, by the access point, the challenge with the first key; and

comparing, by the access point, the authentication information with the challenge encrypted by the access point with the first key to validate the station.

11. (Original) The method of claim 1, wherein the first key is a public key of a public-private key pair for the access point, and the second key is a public key of a public-private key pair for the station.

12. (Original) The method of claim 11 further comprising:

sending, by the access point to the station, the first key; and.

sending, by the station to the access point, the second key.

13. (Original) The method of claim 12, wherein the second key is sent to the access point when the request for the security preference is sent by the station.

14. (Original) The method of claim 12, wherein the first key is sent to the station when the security preference is sent by the access point.

15. (Original) The method of claim 1, wherein establishing the channel creates a standard wired equivalent privacy (WEP) network, and the station and the access point exchange

messages conforming to a format required by the standard that defines a WEP network to establish the WEP network.

16. (Previously presented) A computerized method for connecting a station to a secure wireless network comprising:

sending a request for a security preference through a setup connection to an access point for the secure wireless network, wherein the security preference specifies one authentication protocol from a set of authentication protocols supported by the access point;

generating authentication information for the station when the station receives a security preference specifying shared key from the access point through the setup connection;

sending the authentication information to the access point through the setup connection;

decrypting a channel key in response to receiving an encrypted channel key from the access point through the setup connection; and

sending data encrypted with the channel key to the access point, wherein exchanging data encrypted with the channel key establishes a secure channel in the network.

17. (Original) The method of claim 16 further comprising:

generating a first value using a security algorithm in response to receiving the security preference specifying shared key from the access point;

calculating a self-distributed key using the security algorithm and a second value in response to receiving the second value from the access point; and

using the self-distributed key to generate the authentication information and to decrypt the encrypted channel key.

18. (Original) The method of claim 17, wherein the security algorithm is formulated as $g^n \ mod \ p$ and further comprising:

obtaining integers for y, g and p to generate the first value $Y = g^y \ mod \ p$; and

setting z equal to y^{-1} to calculate the self-distributed key $k = X^z \ mod \ p$.

19. (Original) The method of claim 16 further comprising:

using a first key to generate the authentication information; and

using a second key to decrypt the encrypted channel key.

20. (Original) The method of claim 19, wherein the first key is a public key of a public-private key pair for the access point, and the second key is a private key of a public-private key pair for the station.

21. (Previously presented) A computerized method of securing a wireless network at an access point comprising:

sending a security preference through a setup connection in response to a request from a station, wherein the security preference specifies one authentication protocol from a set of authentication protocols supported by the access point;

validating the station in response to receiving authentication information from the station through the setup connection;

encrypting a channel key when the station is validated;

sending the encrypted channel key to the station through the setup connection; and

sending data encrypted with the channel key to the station, wherein exchanging data encrypted with the channel key establishes a secure channel in the network.

22. (Original) The method of claim 21 further comprising:

generating a self-distributed key using a security algorithm when the security preference is shared key;

generating a second value using the security algorithm and a first value in response to receiving the first value from the station; and

sending the second value to the station.

23. (Original) The method of claim 22, wherein the security algorithm is formulated as $g^n \ mod \ p$ and further comprising:

obtaining integers x, g and p to generate the self-distributed key $k = g^x \ mod \ p$; and

generating the second value $X = Y^x \ mod \ p$.

24. (Original) The method of claim 21 further comprising:

using a first key to evaluate the authentication information; and

using a second key to encrypt the encrypted channel key.

25. (Original) The method of claim 24, wherein the first key is a private key of a public-private key pair for the access point, and the second key is a public key of a public-private key pair for the station.

26. (Previously presented) A computer-readable medium having stored thereon executable instructions to cause a processor to perform a station method to connect to a secure wireless network, the instructions comprising:

sending a request for a security preference through a setup connection to an access point for the secure wireless network, wherein the security preference specifies one authentication protocol from a set of authentication protocols supported by the access point;

generating authentication information for the station when the station receives a security preference specifying shared key from the access point through the setup connection;

sending the authentication information to the access point through the setup connection;

decrypting a channel key in response to receiving an encrypted channel key from the access point through the setup connection; and

sending data encrypted with the channel key to the access point, wherein exchanging data encrypted with the channel key establishes a secure channel in the network.

27. (Original) The computer-readable medium of claim 26 having further instructions comprising:

generating a first value using a security algorithm in response to receiving the security preference specifying shared key from the access point;

calculating a self-distributed key using the security algorithm and a second value in response to receiving the second value from the access point; and

using the self-distributed key to generate the authentication information and to decrypt the encrypted channel key.

28. (Original) The computer-readable medium of claim 27, wherein the security algorithm is formulated as $g^n \bmod p$ and having further instructions comprising:

obtaining integers y, g and p to generate the first value $Y = g^y \bmod p$; and

setting z equal to y^{-1} to calculate the self-distributed key $k = X^z \bmod p$.

29. (Original) The computer-readable medium of claim 26 having further instructions comprising:

using a first key to generate the authentication information; and

using a second key to decrypt the encrypted channel key.

30. (Original) The computer-readable medium of claim 29, wherein the first key is a public key of a public-private key pair for the access point, and the second key is a private key of a public-private key pair for the station.

31. (Previously presented) A computer-readable medium having stored thereon executable instruction to cause a processor to perform an access point method to secure a wireless network, the instructions comprising:

sending a security preference through a setup connection in response to a request from a station, wherein the security preference specifies one authentication protocol from a set of authentication protocols supported by the access point;

validating the station in response to receiving authentication information from the station through the setup connection;

encrypting a channel key when the station is validated;

sending the encrypted channel key to the station through the setup connection; and

sending data encrypted with the channel key to the station, wherein exchanging data encrypted with the channel key establishes a secure channel in the network.

32. (Original) The computer-readable medium of claim 31 having further instructions comprising:

generating a self-distributed key using a security algorithm when the security preference is shared key;

generating a second value using the security algorithm and a first value in response to receiving the first value from the station; and

sending the second value to the station.

33. (Original) The computer-readable medium of claim 32, wherein the security algorithm is formulated as $g^n \bmod p$ and having further instructions comprising:

obtaining integers x, g and p to generate the self-distributed key $k = g^x \bmod p$; and

generating the second value $X = Y^x \bmod p$.

34. (Original) The computer-readable medium of claim 31 having further instructions comprising:

using a first key to evaluate the authentication information; and

using a second key to encrypt the encrypted channel key.

35. (Original) The computer-readable medium of claim 34, wherein the first key is a private key of a public-private key pair for the access point, and the second key is a public key of a public-private key pair for the station.

36. (Previously presented) A secure wireless network comprising:

an access point operable for receiving a connection request from a station through a setup connection, for sending a security preference that specifies one authentication protocol from a set of authentication protocols supported by the access point, for validating authentication information sent by the station, and for connecting the station to the network through a channel secured with a shared channel key; and

a station operable for sending the connection request to the access point, and for generating the authentication information to send to the access point.

37. (Previously Presented) The secure wireless network of claim 36, wherein the access point is further operable for sending a security preference specifying shared key to the station upon receiving the connection request, and the station is operable for sending the authentication information to the access point upon receiving a security preference specifying shared key.

38. (Original) The secure wireless network of claim 37, wherein the access point is further operable for encrypting the shared channel key using a self-distributed key for sending to the station and the station is further operable for decrypting the shared channel key upon receipt.

39. (Original) The secure wireless network of claim 38, wherein the station and the access point are further operable for calculating the self-distributed key by exchanging messages in accordance with the Hughes transmission protocol.

40. (Original) The secure wireless network of claim 36, wherein the station is further operable for using a first key to generate the authentication information and for using a second key to decrypt an encrypted shared channel key received from the access point, and the access point is further operable for using a third key to evaluate the authentication information and for using a fourth key to encrypt the shared channel key for sending to the station.

41. (Original) The secure wireless network of claim 40, wherein the first and third keys are public and private keys, respectively, for the access point, and the second and fourth keys are private and public keys, respectively, for the station.

42. (Previously presented) A computer-readable medium having stored thereon a message data structure for a secure wireless network comprising:

a station address field containing data representing an identifier for a station that exchanges messages with an access point on the secure wireless network;

a transaction sequence number field containing data representing a sequence number for a message exchanged between the station identified by the station address field and the access point;

an authentication algorithm field containing data representing an identifier for one authentication protocol from a set of authentication protocols supported by the access point, the one authentication protocol used by the access point to validate the station identified by the station address field based on a name and password for the station; and

a dependent information field containing data required to connect the station identified by the station address field to the secure wireless network.

43. (Original) The computer-readable medium of claim 42, wherein the data in the dependent information field represents key information for encrypting the name and password for the station identified by the station address field.

44. (Original) The computer-readable medium of claim 42, wherein the data in the dependent information field represents an encrypted name and password for the station identified by the station address field.

45. (Original) The computer-readable medium of claim 42, wherein the data in the dependent information field represents an encrypted channel key used to connect the station identified by the station address field to the secure wireless network.

46. (Previously presented) An apparatus comprising:

a means for accessing a wireless network, the means for accessing operable for receiving a connection request from a means for messaging through a setup connection, for sending a security preference that specifies one authentication protocol from a set of authentication protocols supported by the means for access, for validating authentication information sent by the means for messaging, and for connecting the means for messaging to the wireless network through a channel secured with a shared channel key; and

a means for messaging operable for sending the connection request to the means for accessing, and for generating the authentication information to send to the means for accessing.

47. (Previously presented) The apparatus of claim 46, wherein the means for accessing is further operable for sending a security preference specifying shared key to the means for messaging upon receiving the connection request, and the means for messaging is further

operable for sending the authentication information to the means for accessing upon receiving a security preference specifying shared key.

48. (Previously presented) The apparatus of claim 47, wherein the means for accessing is further operable for encrypting the shared channel key using a self-distributed key for sending to the means for messaging and the means for messaging is further operable for decrypting the shared channel key upon receipt.

49. (Previously presented) The apparatus of claim 48, wherein the means for accessing and the means for messaging are further operable for calculating the self-distributed key by exchanging messages in accordance with the Hughes transmission protocol.

50. (Previously presented) The apparatus of claim 46, wherein the means for messaging is further operable for using a first key to generate the authentication information and for using a second key to decrypt an encrypted shared channel key received from the means for accessing, and the means for accessing is further operable for using a third key to evaluate the authentication information and for using a fourth key to encrypt the shared channel key for sending to the means for messaging.

51. (Previously presented) The apparatus of claim 50, wherein the first and third keys are public and private keys, respectively, for the means for accessing, and the second and fourth keys are private and public keys, respectively, for the means for messaging.

EVIDENCE APPENDIX FOR APPEAL BRIEF UNDER 37 C.F.R. § 41.37

Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, *ANSI/IEEE Std. 802.11*, 1999 Edition, Part 11: pages i-ii, ix-xiv and 59-61.

ANSI/IEEE Std 802.11, 1999 Edition

Information technology— Telecommunications and information exchange between systems— Local and metropolitan area networks— Specific requirements—

Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications

Sponsor

LAN MAN Standards Committee
of the
IEEE Computer Society

ANSI/IEEE Std 802.11, 1999 Edition

IEEE Standards documents are developed within the Technical Committees of the IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Board. Members of the committees serve voluntarily and without compensation. They are not necessarily members of the Institute. The standards developed within IEEE represent a consensus of the broad expertise on the subject within the Institute as well as those activities outside of IEEE that have expressed an interest in participating in the development of the standard.

Use of an IEEE Standard is wholly voluntary. The existence of an IEEE Standard does not imply that there are no other ways to produce, test, measure, purchase, market, or provide other goods and services related to the scope of the IEEE Standard. Furthermore, the viewpoint expressed at the time a standard is approved and issued is subject to change brought about through developments in the state of the art and comments received from users of the standard. Every IEEE Standard is subjected to review at least every five years for revision or reaffirmation. When a document is more than five years old and has not been reaffirmed, it is reasonable to conclude that its contents, although still of some value, do not wholly reflect the present state of the art. Users are cautioned to check to determine that they have the latest edition of any IEEE Standard.

Comments for revision of IEEE Standards are welcome from any interested party, regardless of membership affiliation with IEEE. Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments.

Interpretations: Occasionally questions may arise regarding the meaning of portions of standards as they relate to specific applications. When the need for interpretations is brought to the attention of IEEE, the Institute will initiate action to prepare appropriate responses. Since IEEE Standards represent a consensus of all concerned interests, it is important to ensure that any interpretation has also received the concurrence of a balance of interests. For this reason IEEE and the members of its technical committees are not able to provide an instant response to interpretation requests except in those cases where the matter has previously received formal consideration.

Comments on standards and requests for interpretations should be addressed to:

Secretary, IEEE Standards Board
445 Hoes Lane
P.O. Box 1331
Piscataway, NJ 08855-1331
USA

Note: Attention is called to the possibility that implementation of this standard may require use of subject matter covered by patent rights. By publication of this standard, no position is taken with respect to the existence or validity of any patent rights in connection therewith. The IEEE shall not be responsible for identifying all patents for which a license may be required by an IEEE standard or for conducting inquiries into the legal validity or scope of those patents that are brought to its attention.

The patent holder has, however, filed a statement of assurance that it will grant a license under these rights without compensation or under reasonable rates and nondiscriminatory, reasonable terms and conditions to all applicants desiring to obtain such a license. The IEEE makes no representation as to the reasonableness of rates and/or terms and conditions of the license agreement offered by the patent holder. Contact information may be obtained from the IEEE Standards Department.

Contents

8. Authentication and privacy

8.1 Authentication services

IEEE 802.11 defines two subtypes of authentication service: *Open System* and *Shared Key*. The subtype invoked is indicated in the body of authentication management frames. Thus authentication frames are self-identifying with respect to authentication algorithm. All management frames of subtype Authentication shall be unicast frames as authentication is performed between pairs of stations (i.e., multicast authentication is not allowed). Management frames of subtype Deauthentication are advisory, and may therefore be sent as group-addressed frames.

A mutual authentication relationship shall exist between two stations following a successful authentication exchange as described below. Authentication shall be used between stations and the AP in an infrastructure BSS. Authentication may be used between two STAs in an IBSS.

8.1.1 Open System authentication

Open System authentication is the simplest of the available authentication algorithms. Essentially it is a null authentication algorithm. Any STA that requests authentication with this algorithm may become authenticated if dot11AuthenticationType at the recipient station is set to Open System authentication. Open System authentication is not required to be successful as a STA may decline to authenticate with any particular other STA. Open System authentication is the default authentication algorithm.

Open System authentication involves a two-step authentication transaction sequence. The first step in the sequence is the identity assertion and request for authentication. The second step in the sequence is the authentication result. If the result is "successful," the STAs shall be mutually authenticated.

8.1.1.1 Open System authentication (first frame)

— Message type: Management
— Message subtype: Authentication
— Information items:
  • Authentication Algorithm Identification = "Open System"
  • Station Identity Assertion (in SA field of header)
  • Authentication transaction sequence number = 1
  • Authentication algorithm dependent information (none)
— Direction of message: From authentication initiating STA to authenticating STA

8.1.1.2 Open System authentication (final frame)

— Message type: Management
— Message subtype: Authentication
— Information items:
  • Authentication Algorithm Identification = "Open System"
  • Authentication transaction sequence number = 2
  • Authentication algorithm dependent information (none)
  • The result of the requested authentication as defined in 7.3.1.9
— Direction of message: From authenticating STA to initiating STA

If dot11AuthenticationType does not include the value "Open System," the result code shall not take the value "successful."

8.1.2 Shared Key authentication

Shared Key authentication supports authentication of STAs as either a member of those who know a shared secret key or a member of those who do not. IEEE 802.11 Shared Key authentication accomplishes this without the need to transmit the secret key in the clear; however, it does require the use of the WEP privacy mechanism. Therefore, this authentication scheme is only available if the WEP option is implemented. Additionally, the Shared Key authentication algorithm shall be implemented as one of the dot11AuthenticationAlgorithms at any STA where WEP is implemented.

The required secret, shared key is presumed to have been delivered to participating STAs via a secure channel that is independent of IEEE 802.11. This shared key is contained in a write-only MIB attribute via the MAC management path. The attribute is write-only so that the key value remains internal to the MAC.

During the Shared Key authentication exchange, both the challenge and the encrypted challenge are transmitted. This facilitates unauthorized discovery of the pseudorandom number (PRN) sequence for the key/IV pair used for the exchange. Implementations should therefore avoid using the same key/IV pair for subsequent frames.

A STA shall not initiate a Shared Key authentication exchange unless its dot11PrivacyOptionImplemented attribute is "true."

In the following description, the STA initiating the authentication exchange is referred to as the *requester*, and the STA to which the initial frame in the exchange is addressed is referred to as the *responder*.

8.1.2.1 Shared Key authentication (first frame)

— Message type: Management
— Message subtype: Authentication
— Information Items:
  • Station Identity Assertion (in SA field of header)
  • Authentication Algorithm Identification = "Shared Key"
  • Authentication transaction sequence number = 1
  • Authentication algorithm dependent information (none)
— Direction of message: From requester to responder

8.1.2.2 Shared Key authentication (second frame)

Before sending the second frame in the Shared Key authentication sequence, the responder shall use WEP to generate a string of octets that shall be used as the authentication challenge text.

— Message type: Management
— Message subtype: Authentication
— Information Items:
  • Authentication Algorithm Identification = "Shared Key"
  • Authentication transaction sequence number = 2
  • Authentication algorithm dependent information = the authentication result.
  • The result of the requested authentication as defined in 7.3.1.9

    If the status code is not "successful," this shall be the last frame of the transaction sequence. If the status code is not "successful," the content of the challenge text field is unspecified.

    If the status code is "successful," the following additional information items shall have valid contents:

    Authentication algorithm dependent information = challenge text.

This field shall be of fixed length of 128 octets. The field shall be filled with octets generated by the WEP pseudo-random number generator (PRNG). The actual value of the challenge field is unimportant, but the value shall not be a single static value. The key and IV used when generating the challenge text are unspecified because this key/IV value does not have to be shared and does not affect interoperability.

— Direction of message: From responder to requester

8.1.2.3 Shared Key authentication (third frame)

The requester shall copy the challenge text from the second frame into the third frame. The third frame shall be transmitted after encryption by WEP, as defined in 8.2.3, using the shared secret key.

— Message type: Management
— Message subtype: Authentication
— Information Items:
  • Authentication Algorithm Identification = "Shared Key"
  • Authentication transaction sequence number = 3
  • Authentication algorithm dependent information = challenge text from sequence two frame
— Direction of message: From requester to responder

This frame shall be encrypted as described below.

8.1.2.4 Shared Key authentication (final frame)

The responder shall attempt to decrypt the contents of the third frame in the authentication sequence as described below. If the WEP ICV check is successful, the responder shall then compare the decrypted contents of the Challenge Text field to the challenge text that was sent in Frame 2 of the sequence. If they are the same, then the responder shall respond with a successful status code in Frame 4 of the sequence. If the WEP ICV check fails, the responder shall respond with an unsuccessful status code in Frame 4 of the sequence as described below.

— Message type: Management
— Message subtype: Authentication
— Information Items:
  • Authentication Algorithm Identification = "Shared Key"
  • Authentication transaction sequence number = 4
  • Authentication algorithm dependent information = the authentication result
    The result of the requested authentication.
    This is a fixed length item with values "successful" and "unsuccessful."
— Direction of message: From responder to requester

8.2 The Wired Equivalent Privacy (WEP) algorithm

8.2.1 Introduction

Eavesdropping is a familiar problem to users of other types of wireless technology. IEEE 802.11 specifies a wired LAN equivalent data confidentiality algorithm. *Wired equivalent privacy* is defined as protecting authorized users of a wireless LAN from casual eavesdropping. This service is intended to provide functionality for the wireless LAN equivalent to that provided by the physical security attributes inherent to a wired medium.

Data confidentiality depends on an external key management service to distribute data enciphering/deciphering keys. The IEEE 802.11 standards committee specifically recommends against running an IEEE 802.11

RELATED PROCEEDINGS APPENDIX FOR APPEAL BRIEF UNDER 37 C.F.R. § 41.37

NONE